UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/823,491	03/31/2001	James W. Edwards	042390P10503	6546

7590   11/03/2004

Michael A. DeSanctis
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER
PYZOCHA, MICHAEL J

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 11/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/823,491	EDWARDS ET AL.
	Examiner	**Art Unit**	
	Michael Pyzocha	2137	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>31 March 2001</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-33</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-33</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>31 March 2004</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1. Claims 1-33 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which

forms the basis for all obviousness rejections set forth in this

Office action:

> (a) A patent may not be obtained though the invention is not identically
> disclosed or described as set forth in section 102 of this title, if the
> differences between the subject matter sought to be patented and the prior
> art are such that the subject matter as a whole would have been obvious at
> the time the invention was made to a person having ordinary skill in the
> art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

3. Claims 1, 12, 23 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Kettlewell (webpage), and further in

view of Koopman (webpage).

As per claims 1, 12, and 23, Kettlewell discloses the

method, apparatus and medium for executing a modified call

routine for placing a random amount of empty space onto a stack

(see page 3), executing a called function (see page 4).

Kettlewell fails to disclose a modified return routine for

removing said random amount of empty space from the stack.

However, Koopman teaches removing data from a stack (see

pages 1-2).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Koppman's method of removing data from a stack to remove the random space of Kettlewell.

Motivation to do so would have been to prevent the stack from overflowing (see Koopman Figure 1.1 where after 9 is pushed onto the stack if it is not removed the stack will overflow).

4.   Claims 2-4, 8-11, 13-15, 19-22, 24-26, 30-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Kettlewell and Koopman system as applied to claims 1, 12, 23 above, and further in view of Cowan et al (webpage).

As per claims 2, 13, and 24, the modified Kettlewell and Koopman system discloses calculating a random number; saving said random number in a secure location; placing a plurality of blank bytes equal to the random number onto the stack (Kettlewell page 3); and setting an end of stack pointer to an end of the stack frame (see Koopman page 2 section 1.2.2 paragraph 1).

The modified Kettlewell and Koopman system fails to disclose placing a return address for the called function on the stack; and building a stack frame by placing values from the called function onto the stack.

However Cowan et al teaches placing a return address for the called function on the stack (see Cowan et al page 7 figure 2); building a stack frame by placing values from the called function onto the stack (see Cowan et al figure 2).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Cowan et al's method of adding the return address onto the stack and building a stack from in the modified system of Kettlewell and Koopman.

Motivation to do so would have been to allow the stack to return to its original location (see Cowan et al page 4).

As per claims 3, 14, and 25, the modified Kettlewell, Koopman and Cowan et al system discloses the secure location being a register not generally accessible (see Cowan et al figure 3)

As per claims 4, 15, and 26, the modified Kettlewell, Koopman and Cowan et al system discloses the modified return routine comprises: recalling a random number saved during an execution of said modified call routine (see Cowan et al figure 4 line 1 where the canary is the random space of Kettlewell); removing a number of bytes equal to said random number from the stack (see Cowan et al figure 4 line 3); retrieving a return address for the called function from the stack (see Cowan et al page 7 first paragraph); and setting an end of stack pointer to

an end of a previous stack frame (see Koopman page 2 section

1.2.2 paragraph 1).

As per claims 8, 19, and 30, the modified Cowan et al and

Koopman system discloses searching an executable program for all

function calls at the time the executable is installed; adding a

random amount of blank space to all stacks generated by said

function calls (see Kettlewell page 3); adjusting all references

to said stacks to compensate for said blank space (see Koopman

page 2 section 1.2.2 paragraph 1).

As per claims 9-11, 20-22, and 31-33, the modified Cowan et

al and Koopman system discloses the method is performed when the

executable is installed or loaded and saving the executable (see

Cowan et al page 8 where running a program through the compiler

is a way of installation and it is inherent that the compiler

will at least temporarily save the outputted executable).

5.   Claims 5-7, 16-18, 27-29 are rejected under 35

U.S.C. 103(a) as being unpatentable over the modified

Kettlewell, Koopman and Cowan et al system as applied to claims

1, 12, 23 above, and further in view of Menezes et al (Handbook

of Applied Cryptography).

As per claims 5, 16, and 27 the modified Kettlewell,

Koopman and Cowan et al system discloses placing a return

address for the called function on the stack (see Cowan et al

figure 2) and building a stack frame by placing values from the

called function onto the stack (see Cowan et al figure 2).

The modified Kettlewell, Koopman and Cowan et al system

fails to disclose calculating a hash value and storing a hash

value of the stack invariants.

However, Menezes et al teaches the use of hash values for

message integrity (see page 323 and it is inherent that the hash

must be done on invariants and that it must be stored in order

to check the integrity).

At the time of the invention it would have been obvious to

a person of ordinary skill in the art to use Menezes et al's

hash function in the modified Kettlewell, Koopman and Cowan et

al system.

Motivation to do so would have been to provide content

integrity (see Menezes et al page 323)

As per claims 6, 17, and 28, the modified Kettlewell,

Koopman, Cowan et al and Menezes et al system discloses the

secure location is a processor register that is not generally

accessible (see Cowan et al figure 3).

As per claims 7, 18, and 29, the modified Kettlewell,

Koopman, Cowan et al and Menezes et al system discloses

calculating a second hash value of stack invariants; determining

whether said second hash value matches a first hash value

calculated during an execution of said modified call routine

(see Menezes et al page 323); executing a stack corruption

exception if said second hash value does not match said first

hash value; and setting an end of stack pointer to an end of a

previous stack frame if said second hash value matches said

first hash value (see Cowan et al figure 4).

Conclusion

Any inquiry concerning this communication or earlier

communications from the examiner should be directed to Michael

Pyzocha whose telephone number is (571) 272-3875. The examiner

can normally be reached on 7:00am - 4:30pm first Fridays of the

bi-week off.

If attempts to reach the examiner by telephone are

unsuccessful, the examiner's supervisor, Andrew Caldwell can be

reached on (571) 272-3868. The fax phone number for the

organization where this application or proceeding is assigned is

703-872-9306.

Information regarding the status of an application may be
obtained from the Patent Application Information Retrieval
(PAIR) system. Status information for published applications
may be obtained from either Private PAIR or Public PAIR. Status
information for unpublished applications is available through
Private PAIR only. For more information about the PAIR system,
see http://pair-direct.uspto.gov. Should you have questions on
access to the Private PAIR system, contact the Electronic
Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

MJP